



BURKINA FASO COMPUTER INCIDENT RESPONSE TEAM

Committed to reducing the vulnerability of cyberspace, Incident Management and strengthening the culture of cybersecurity

Security newsletter for the week of March 24, 2014

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player 12.0.0.77 on Windows allows remote attackers to execute arbitrary code and bypass an Internet Explorer sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.	2014-03-27	10.0	CVE-2014-0506
adobe -- flash_player	Heap-based buffer overflow in Adobe Flash Player 12.0.0.77 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by Zeguang Zhao and Liang Chen during a Pwn2Own competition at CanSecWest 2014.	2014-03-27	10.0	CVE-2014-0510
adobe -- acrobat_reader	Heap-based buffer overflow in Adobe Reader 11.0.06 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.	2014-03-27	10.0	CVE-2014-0511
adobe -- acrobat_reader	Adobe Reader 11.0.06 allows attackers to bypass a PDF sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.	2014-03-27	10.0	CVE-2014-0512
apache -- camel	The XSLT component in Apache Camel 2.11.x before 2.11.4, 2.12.x before 2.12.3, and possibly earlier versions allows remote attackers to execute arbitrary Java methods via a crafted message.	2014-03-21	7.5	CVE-2014-0003
apple -- safari	Unspecified vulnerability in Apple Safari 7.0.2 on OS X allows remote	2014-03-26	10.0	CVE-2014-1300

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to execute arbitrary code with root privileges via unknown vectors, as demonstrated by Google during a Pwn4Fun competition at CanSecWest 2014.			
apple -- safari	Heap-based buffer overflow in Apple Safari 7.0.2 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by Liang Chen during a Pwn2Own competition at CanSecWest 2014.	2014-03-26	10.0	CVE-2014-1303
b-e-soft -- artweaver_free	Stack-based buffer overflow in Artweaver Plus and Free before 3.1.5 allows remote attackers to execute arbitrary code via a crafted JPG image file.	2014-03-27	9.3	CVE-2013-3481
cisco -- ios	Cisco IOS 15.3M before 15.3(3)M2 and IOS XE 3.10.xS before 3.10.2S allow remote attackers to cause a denial of service (device reload) via crafted SIP messages, aka Bug ID CSCug45898.	2014-03-27	7.8	CVE-2014-2106
cisco -- ios	Cisco IOS 12.2 and 15.0 through 15.3, when used with the Kailash FPGA before 2.6 on RSP720-3C-10GE and RSP720-3CXL-10GE devices, allows remote attackers to cause a denial of service (route switch processor outage) via crafted IP packets, aka Bug ID CSCug84789.	2014-03-27	7.1	CVE-2014-2107
cisco -- ios	Cisco IOS 12.2 and 15.0 through 15.3 and IOS XE 3.2 through 3.7 before 3.7.5S and 3.8 through 3.10 before 3.10.1S allow remote attackers to cause a denial of service (device reload) via a malformed IKEv2 packet, aka Bug ID CSCui88426.	2014-03-27	7.8	CVE-2014-2108
cisco -- ios	The TCP Input module in Cisco IOS 12.2 through 12.4 and 15.0 through 15.4, when NAT is used, allows remote attackers to cause a denial of service (memory consumption or device reload) via crafted TCP packets, aka Bug IDs CSCuh33843 and CSCuj41494.	2014-03-27	7.8	CVE-2014-2109
cisco -- ios	The Application Layer Gateway (ALG) module in Cisco IOS 12.2 through 12.4 and 15.0 through 15.4, when NAT is used, allows remote attackers to cause	2014-03-27	7.1	CVE-2014-2111

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a denial of service (device reload) via crafted DNS packets, aka Bug ID CSCue00996.			
cisco -- ios	The SSL VPN (aka WebVPN) feature in Cisco IOS 15.1 through 15.4 allows remote attackers to cause a denial of service (memory consumption) via crafted HTTP requests, aka Bug ID CSCuf51357.	2014-03-27	7.8	CVE-2014-2112
cisco -- ios	Cisco IOS 15.1 through 15.3 and IOS XE 3.3 and 3.5 before 3.5.2E; 3.7 before 3.7.5S; and 3.8, 3.9, and 3.10 before 3.10.2S allow remote attackers to cause a denial of service (I/O memory consumption and device reload) via a malformed IPv6 packet, aka Bug ID CSCui59540.	2014-03-27	7.8	CVE-2014-2113
gplhost -- domain_technologie_control	The drawAdminTools_PackageInstaller function in shared/inc/forms/packager.php in Domain Technologie Control (DTC) before 0.32.11 allows remote attackers to execute arbitrary commands via shell metacharacters in the dtcpkg_directory parameter in a do_install action to dtc/.	2014-03-21	7.5	CVE-2011-5274
ibm -- datacap_taskmaster_capture	Stack-based buffer overflow in the Taskmaster Capture ActiveX control in IBM Datacap Taskmaster Capture 8.0.1, and 8.1 before FP2, allows remote attackers to execute arbitrary code via unspecified vectors.	2014-03-21	9.3	CVE-2014-0879
ibm -- lotus_protector_for_mail_security	The Admin Web UI in IBM Lotus Protector for Mail Security 2.8.x before 2.8.1-22905 allows remote authenticated users to bypass intended access restrictions and execute arbitrary commands via unspecified vectors.	2014-03-25	7.1	CVE-2014-0886
ibm -- lotus_protector_for_mail_security	The Admin Web UI in IBM Lotus Protector for Mail Security 2.8.x before 2.8.1-22905 allows remote authenticated users to execute arbitrary commands with root privileges via unspecified vectors.	2014-03-25	7.1	CVE-2014-0887
ibm -- security_appscan	The update process in IBM Security AppScan Standard 7.9 through 8.8 does not require integrity checks of downloaded files, which allows remote	2014-03-26	7.6	CVE-2014-0904

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to execute arbitrary code via a crafted file.			
kingsoft -- office_2012	Stack-based buffer overflow in wpsio.dll in Kingsoft WPS Office 2012 possibly 8.1.0.3238 allows remote attackers to execute arbitrary code via a long BSTR string.	2014-03-24	10.0	CVE-2012-4886
linux -- linux_kernel	net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) dccp_new, (2) dccp_packet, or (3) dccp_error function.	2014-03-24	10.0	CVE-2014-2523
maygion -- ip_camera_firmware	Buffer overflow in MayGion IP Cameras with firmware before 2013.04.22 (05.53) allows remote attackers to execute arbitrary code via a long filename in a GET request.	2014-03-25	7.5	CVE-2013-1605
microsoft -- office	Microsoft Word 2003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT; Word Viewer; Office Compatibility Pack SP3; Office for Mac 2011; Word Automation Services on SharePoint Server 2010 SP1 and SP2 and 2013; Office Web Apps 2010 SP1 and SP2; and Office Web Apps Server 2013 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data, as exploited in the wild in March 2014.	2014-03-25	9.3	CVE-2014-1761
nuance -- pdf_reader	Heap-based buffer overflow in PDFCore8.dll in Nuance PDF Reader before 8.1 allows remote attackers to execute arbitrary code via crafted font table directory values in a TTF file, related to naming table entries.	2014-03-27	9.3	CVE-2013-0732
siemens -- simatic_s7_cpu-1211c	The random-number generator on Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 does not have sufficient entropy, which makes it easier for remote attackers to defeat cryptographic protection mechanisms and hijack sessions via unspecified vectors, a different vulnerability than CVE-2014-2251.	2014-03-24	8.3	CVE-2014-2250
siemens -- simatic_s7_cpu-1211c	Siemens SIMATIC S7-1200 CPU PLC	2014-03-24	7.8	CVE-2014-2254

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets, a different vulnerability than CVE-2014-2255.			
siemens -- simatic_s7_cpu-1211c	Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted ISO-TSAP packets, a different vulnerability than CVE-2014-2257.	2014-03-24	7.8	CVE-2014-2256
siemens -- simatic_s7_cpu-1211c	Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted HTTPS packets, a different vulnerability than CVE-2014-2259.	2014-03-24	7.8	CVE-2014-2258

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
barracudadrive -- barracudadrive	Multiple cross-site scripting (XSS) vulnerabilities in BarracudaDrive before 6.7 allow remote attackers to inject arbitrary web script or HTML via the (1) sForumName or (2) sDescription parameter to Forum/manage/ForumManager.lsp; (3) sHint, (4) sWord, or (5) nId parameter to Forum/manage/hangman.lsp; (6) user parameter to rtl/protected/admin/wizard/setuser.lsp; (7) name or (8) email parameter to feedback.lsp; (9) lname or (10) url parameter to private/manage/PageManager.lsp; (11) cmd parameter to fs; (12) newname, (13) description, (14) firstname, (15) lastname, or (16) id parameter to rtl/protected/mail/manage/list.lsp; or (17) PATH_INFO to fs/.	2014-03-25	4.3	CVE-2014-2526
cacti -- cacti	Cross-site scripting (XSS) vulnerability in Cacti 0.8.7g allows remote attackers to inject arbitrary web script or HTML via	2014-03-27	4.3	CVE-2014-2326

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unspecified vectors.			
christos_zoulas -- file	The BEGIN regular expression in the awk script detector in magic/Magdir/commands in file before 5.15 uses multiple wildcards with unlimited repetitions, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted ASCII file that triggers a large amount of backtracking, as demonstrated via a file with many newline characters.	2014-03-24	5.0	CVE-2013-7345
cisco -- prime_security_manager	Multiple cross-site scripting (XSS) vulnerabilities in dashboard-related HTML documents in Cisco Prime Security Manager (aka PRSM) 9.2(.1-2) and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified parameters, aka Bug ID CSCun50687.	2014-03-27	4.3	CVE-2014-2118
dell -- sonicwall_network_security_appliance_2400	Cross-site scripting (XSS) vulnerability in the Dashboard Backend service (stats/dashboard.jsp) in SonicWall Network Security Appliance (NSA) 2400 allows remote attackers to inject arbitrary web script or HTML via the sn parameter.	2014-03-24	4.3	CVE-2014-2589
emc -- rsa_bsafe	The server in EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x before 4.0.5 does not properly process certificate chains, which allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	2014-03-25	5.0	CVE-2014-0628
flowplayer -- flowplayer_flash	Multiple cross-site scripting (XSS) vulnerabilities in Flowplayer Flash before 3.2.17, as used in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2, allow remote attackers to inject arbitrary web script or HTML by (1) providing a crafted playerId or (2) referencing an external domain, a related issue to CVE-2013-7342.	2014-03-24	4.3	CVE-2013-7341
flowplayer -- flowplayer_html5	Cross-site scripting (XSS) vulnerability in flowplayer.swf in the Flash fallback feature in Flowplayer HTML5 5.4.1 allows remote attackers to inject arbitrary web script or HTML via the callback parameter, a related issue to CVE-2013-7341.	2014-03-24	4.3	CVE-2013-7342

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flowplayer -- flowplayer_html5	Cross-site scripting (XSS) vulnerability in flowplayer.swf in the Flash fallback feature in Flowplayer HTML5 5.4.3 allows remote attackers to inject arbitrary web script or HTML by using URL encoding within the callback parameter name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-7342.	2014-03-24	4.3	CVE-2013-7343
gplhost -- domain_technologie_control	SQL injection vulnerability in Domain Technologie Control (DTC) before 0.34.1 allows remote authenticated users to execute arbitrary SQL commands via the addrlink parameter to shared/inc/forms/domain_info.php. NOTE: CVE-2011-3197 has been SPLIT due to findings by different researchers. CVE-2011-5272 has been assigned for the vps_note parameter to dtcadmin/logPushlet.php vector.	2014-03-21	6.5	CVE-2011-3197
gplhost -- domain_technologie_control	SQL injection vulnerability in Domain Technologie Control (DTC) before 0.34.1 allows remote authenticated users to execute arbitrary SQL commands via the vps_note parameter to dtcadmin/logPushlet.php. NOTE: this issue was originally part of CVE-2011-3197, but that ID was SPLIT due to different researchers.	2014-03-21	6.5	CVE-2011-5272
ibm -- infosphere_biginsights	Open redirect vulnerability in the Web Application Enterprise Console in IBM InfoSphere BigInsights 1.1 and 2.x before 2.1 FP2 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2014-03-26	4.9	CVE-2013-3997
ibm -- websphere_mq_internet_pass_thru	The command-port listener in IBM WebSphere MQ Internet Pass-Thru (MQIPT) 2.x before 2.1.0.1 allows remote attackers to cause a denial of service (remote-administration outage) via unspecified vectors.	2014-03-21	5.0	CVE-2013-5401
ibm -- cognos_express	Cross-site request forgery (CSRF) vulnerability in IBM Cognos Express 9.0 before IFIX 2, 9.5 before IFIX 2, 10.1 before IFIX 2, and 10.2.1 before FP1 allows remote attackers to hijack the authentication of arbitrary users.	2014-03-25	6.8	CVE-2013-5443
ibm -- cognos_express	The server in IBM Cognos Express 9.0	2014-03-25	5.0	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	before IFIX 2, 9.5 before IFIX 2, 10.1 before IFIX 2, and 10.2.1 before FP1 allows remote attackers to read encrypted credentials via unspecified vectors.			2013-5444
ibm -- cognos_express	IBM Cognos Express 9.0 before IFIX 2, 9.5 before IFIX 2, 10.1 before IFIX 2, and 10.2.1 before FP1 allows local users to obtain sensitive cleartext information by leveraging knowledge of a static decryption key.	2014-03-25	5.0	CVE-2013-5445
ibm -- rational_clearcase	Multiple buffer overflows in IBM Rational ClearCase 7.x before 7.1.2.13, 8.0.0.x before 8.0.0.10, and 8.0.1.x before 8.0.1.3 allow remote authenticated users to obtain privileged access via unspecified vectors.	2014-03-21	6.5	CVE-2014-0829
ibm -- lotus_protector_for_mail_security	Cross-site request forgery (CSRF) vulnerability in the Admin Web UI in IBM Lotus Protector for Mail Security 2.8.x before 2.8.1-22905 allows remote authenticated users to hijack the authentication of unspecified victims via unknown vectors.	2014-03-25	6.8	CVE-2014-0885
icinga -- icinga	Multiple off-by-one errors in Icinga, possibly 1.10.2 and earlier, allow remote attackers to cause a denial of service (crash) via unspecified vectors to the (1) display_nav_table, (2) print_export_link, (3) page_num_selector, or (4) page_limit_selector function in cgi/cgiutils.c or (5) status_page_num_selector function in cgi/status.c, which triggers a stack-based buffer overflow.	2014-03-25	5.0	CVE-2014-2386
ithoughts -- ithoughtshd	The iThoughtsHD app 4.19 for iOS on iPad devices, when the WiFi Transfer feature is used, allows remote attackers to upload arbitrary files by placing a %00 sequence after a dangerous extension, as demonstrated by a .html%00.txt file.	2014-03-26	4.3	CVE-2014-1827
ithoughts -- ithoughtshd	The iThoughts web server in the iThoughtsHD app 4.19 for iOS on iPad devices allows remote attackers to cause a denial of service (disk consumption) by uploading a large file.	2014-03-26	4.3	CVE-2014-1828
joshua_peek -- rack-ssl	Cross-site scripting (XSS) vulnerability in lib/rack/ssl.rb in the rack-ssl gem before 1.4.0 for Ruby allows remote	2014-03-25	4.3	CVE-2014-2538

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to inject arbitrary web script or HTML via a URI, which might not be properly handled by third-party adapters such as JRuby-Rack.			
linux -- linux_kernel	The rds_ib_laddr_check function in net/rds/ib.c in the Linux kernel before 3.12.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a bind system call for an RDS socket on a system that lacks RDS transports.	2014-03-24	4.7	CVE-2013-7339
maygion -- ip_camera_firmware	Directory traversal vulnerability in MayGion IP Cameras with firmware before 2013.04.22 (05.53) allows remote attackers to read arbitrary files via a .. (dot dot) in the default URI.	2014-03-25	5.0	CVE-2013-1604
mcafee -- cloud_single_sign_on	Cross-site scripting (XSS) vulnerability in the login audit form in McAfee Cloud Single Sign On (SSO) allows remote attackers to inject arbitrary web script or HTML via a crafted password.	2014-03-24	4.3	CVE-2014-2586
mcafee -- asset_manager	SQL injection vulnerability in jsp/reports/ReportsAudit.jsp in McAfee Asset Manager 6.6 allows remote authenticated users to execute arbitrary SQL commands via the username of an audit report (aka user parameter).	2014-03-24	6.5	CVE-2014-2587
mcafee -- asset_manager	Directory traversal vulnerability in servlet/downloadReport in McAfee Asset Manager 6.6 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the reportFileName parameter.	2014-03-24	4.0	CVE-2014-2588
moodle -- moodle	mod/chat/chat_ajax.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 does not properly check for the mod/chat:chat capability during chat sessions, which allows remote authenticated users to bypass intended access restrictions in opportunistic circumstances by remaining in a chat session after an intra-session capability removal by an administrator.	2014-03-24	4.9	CVE-2014-0122
moodle -- moodle	The wiki subsystem in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 does not properly restrict (1) view and (2) edit	2014-03-24	4.9	CVE-2014-0123

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access, which allows remote authenticated users to perform wiki operations by leveraging the student role and using the Recent Activity block to reach the individual wiki of an arbitrary student.			
moodle -- moodle	The identity-reporting implementations in mod/forum/renderer.php and mod/quiz/override_form.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 do not properly restrict the display of e-mail addresses, which allows remote authenticated users to obtain sensitive information by using the (1) Forum or (2) Quiz module.	2014-03-24	4.0	CVE-2014-0124
moodle -- moodle	repository/alfresco/lib.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 places a session key in a URL, which allows remote attackers to bypass intended Alfresco Repository file restrictions by impersonating a file's owner.	2014-03-24	5.8	CVE-2014-0125
moodle -- moodle	Cross-site request forgery (CSRF) vulnerability in enrol/imsenterprise/importnow.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote attackers to hijack the authentication of administrators for requests that import an IMS Enterprise file.	2014-03-24	6.8	CVE-2014-0126
moodle -- moodle	The time-validation implementation in (1) mod/feedback/complete.php and (2) mod/feedback/complete_guest.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote authenticated users to bypass intended restrictions on starting a Feedback activity by choosing an unavailable time.	2014-03-24	4.9	CVE-2014-0127
moodle -- moodle	badges/mybadges.php in Moodle 2.5.x before 2.5.5 and 2.6.x before 2.6.2 does not properly track the user to whom a badge was issued, which allows remote authenticated users to modify the visibility of an arbitrary badge via unspecified vectors.	2014-03-24	4.0	CVE-2014-0129

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moodle -- moodle	mod/assign/externallib.php in Moodle 2.6.x before 2.6.2 does not properly handle assignment web-service parameters, which might allow remote authenticated users to modify grade metadata via unspecified vectors.	2014-03-24	4.0	CVE-2014-2572
mozilla -- network_security_services	The cert_TestHostName function in lib/certdb/certdb.c in the certificate-checking implementation in Mozilla Network Security Services (NSS) before 3.16 accepts a wildcard character that is embedded in an internationalized domain name's U-label, which might allow man-in-the-middle attackers to spoof SSL servers via a crafted certificate.	2014-03-25	4.3	CVE-2014-1492
net-snmp -- net-snmp	The Linux implementation of the ICMP-MIB in Net-SNMP 5.5 before 5.5.2.1, 5.6.x before 5.6.2.1, and 5.7.x before 5.7.2.1 does not properly validate input, which allows remote attackers to cause a denial of service via unspecified vectors.	2014-03-24	5.0	CVE-2014-2284
openbsd -- openssh	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.	2014-03-27	5.8	CVE-2014-2653
opensolution -- quick_cart	Cross-site scripting (XSS) vulnerability in Open Solution Quick.Cms 5.0 and Quick.Cart 6.0, possibly as downloaded before December 19, 2012, allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to admin.php. NOTE: this might be a duplicate of CVE-2008-4140.	2014-03-24	4.3	CVE-2012-6430
openssl -- openssl	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.	2014-03-25	4.3	CVE-2014-0076
owncloud -- owncloud	Unspecified vulnerability in core/ajax/translations.php in ownCloud before 4.0.12 and 4.5.x before 4.5.6 allows remote authenticated users to execute arbitrary PHP code via unknown vectors. NOTE: this entry has been SPLIT due to different affected versions.	2014-03-24	6.5	CVE-2013-0303

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The core/settings.php issue is covered by CVE-2013-7344.			
owncloud -- owncloud	Unspecified vulnerability in core/settings.php in ownCloud before 4.0.12 and 4.5.x before 4.5.6 allows remote authenticated users to execute arbitrary PHP code via unknown vectors. NOTE: this issue was SPLIT from CVE-2013-0303 due to different affected versions.	2014-03-24	6.5	CVE-2013-7344
owncloud -- owncloud	Multiple cross-site scripting (XSS) vulnerabilities in ownCloud before 6.0.2 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-03-24	4.3	CVE-2014-2057
owncloud -- owncloud	ownCloud before 5.0.15 and 6.x before 6.0.2, when the file_external app is enabled, allows remote authenticated users to mount the local filesystem in the user's ownCloud via the mount configuration.	2014-03-24	4.9	CVE-2014-2585
oxid-esales -- eshop	Multiple cross-site scripting (XSS) vulnerabilities in OXID eShop Professional and Community Edition 4.6.8 and earlier, 4.7.x before 4.7.11, and 4.8.x before 4.8.4, and Enterprise Edition 4.6.8 and earlier, 5.0.x before 5.0.11 and 5.1.x before 5.1.4 allow remote attackers to inject arbitrary web script or HTML via the searchtag parameter to the getTag function in (1) application/controllers/details.php or (2) application/controllers/tag.php.	2014-03-25	4.3	CVE-2014-2016
php -- php	The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.	2014-03-21	4.3	CVE-2014-2497
redhat -- enterprise_linux	The get_rx_bufs function in drivers/vhost/net.c in the vhost-net subsystem in the Linux kernel package before 2.6.32-431.11.2 on Red Hat Enterprise Linux (RHEL) 6 does not properly handle vhost_get_vq_desc errors, which allows guest OS users to cause a denial of service (host OS crash) via unspecified vectors.	2014-03-26	5.5	CVE-2014-0055

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rsa -- authentication_manager	Cross-site scripting (XSS) vulnerability in the Self-Service Console in EMC RSA Authentication Manager 7.1 before SP4 P32 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to a "cross frame scripting" issue.	2014-03-27	4.3	CVE-2014-0623
siemens -- simatic_s7_cpu-1211c	Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted PROFINET packets, a different vulnerability than CVE-2014-2253.	2014-03-24	6.1	CVE-2014-2252
stunnel -- stunnel	stunnel before 5.00, when using fork threading, does not properly update the state of the OpenSSL pseudo-random number generator (PRNG), which causes subsequent children with the same process ID to use the same entropy pool and allows remote attackers to obtain private keys for EC (ECDSA) or DSA certificates.	2014-03-24	4.3	CVE-2014-0016
symphony-cms -- symphony_cms	SQL injection vulnerability in Symphony CMS before 2.3.2 allows remote authenticated users to execute arbitrary SQL commands via the sort parameter to system/authors/. NOTE: this can be leveraged using CSRF to allow remote unauthenticated attackers to execute arbitrary SQL commands.	2014-03-27	6.5	CVE-2013-2559
symphony-cms -- symphony_cms	Cross-site request forgery (CSRF) vulnerability in Symphony CMS before 2.3.2 allows remote attackers to hijack the authentication of administrators for requests that conduct SQL injection attacks via the sort parameter to system/authors/, related to CVE-2013-2559.	2014-03-27	6.8	CVE-2013-7346
theforeman -- foreman	Cross-site scripting (XSS) vulnerability in app/views/common/500.html.erb in Foreman 1.4.x before 1.4.2 allows remote authenticated users to inject arbitrary web script or HTML via the bookmark name when adding a bookmark.	2014-03-27	4.3	CVE-2014-0089
trojita_project -- trojita	The OpenConnectionTask::handleStateHelper function in Imap/Tasks/OpenConnectionTask.cpp in	2014-03-21	4.3	CVE-2014-2567

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Trojita before 0.4.1 allows man-in-the-middle attackers to trigger use of cleartext for saving a message into a (1) sent or (2) draft folder via a PREAUTH response that prevents later use of the STARTTLS command.			
videolan -- vlc_media_player	VideoLAN VLC Media Player before 2.0.7 allows remote attackers to cause a denial of service (memory consumption) via a crafted playlist file.	2014-03-21	4.3	CVE-2013-7340
virtualaccess -- gw6110a	The web interface on Virtual Access GW6110A routers with software 9.00 before 9.09.27, 9.50 before 9.50.21, and 10.00 before 10.00.21 allows remote authenticated users to gain privileges via a modified JavaScript variable.	2014-03-25	4.9	CVE-2014-0343
wysija_newsletters_project -- wysija_newsletters	Multiple SQL injection vulnerabilities in the Wysija Newsletters plugin before 2.2.1 for WordPress allow remote authenticated administrators to execute arbitrary SQL commands via the (1) search or (2) orderby parameter to wp-admin/admin.php. NOTE: this can be leveraged using CSRF to allow remote unauthenticated attackers to execute arbitrary SQL commands.	2014-03-24	6.5	CVE-2013-1408

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
extplorer -- extplorer	Multiple cross-site scripting (XSS) vulnerabilities in eXtplorer 2.1.3, when used as a component for Joomla!, allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) application.js.php in scripts/ or (2) admin.php, (3) copy_move.php, (4) functions.php, (5) header.php, or (6) upload.php in include/.	2014-03-25	2.6	CVE-2013-5951
gplhost -- domain_technologie_control	The setup script in Domain Technologie Control (DTC) before 0.34.1 uses world-readable permissions for	2014-03-21	2.1	CVE-2011-3196

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/etc/apache2/apache2.conf, which allows local users to obtain the dtcdaemons MySQL password by reading the file.			
gplhost -- domain_technologie_control	Multiple cross-site scripting (XSS) vulnerabilities in Domain Technologie Control (DTC) before 0.34.1 allow remote authenticated users to inject arbitrary web script or HTML via the (1) message body of a support ticket or unspecified vectors to the (2) DNS and (3) MX form, as demonstrated by the "Domain root TXT record:" field.	2014-03-21	3.5	CVE-2011-3199
ibm -- data_protection	The (1) Data Protection for Exchange component 6.1 before 6.1.3.4 and 6.3 before 6.3.1 in IBM Tivoli Storage Manager for Mail and the (2) FlashCopy Manager for Exchange component 2.2 and 3.1 before 3.1.1 in IBM Tivoli Storage FlashCopy Manager do not properly constrain mailbox contents during certain PST restore operations, which allows remote authenticated users to read the personal e-mail of other users in opportunistic circumstances by launching an e-mail client after an administrator performs a multiple-mailbox restore.	2014-03-26	2.1	CVE-2013-3976
ibm -- infosphere_biginsights	CRLF injection vulnerability in the Web Application Enterprise Console in IBM InfoSphere BigInsights 1.1 and 2.x before 2.1 FP2 allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors.	2014-03-26	3.5	CVE-2013-3998
ibm -- quickfile	Cross-site scripting (XSS) vulnerability in IBM QuickFile 1.0.0.0 before iFix 4 and 1.1.0.1 before iFix 3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.	2014-03-21	3.5	CVE-2013-6729
ibm -- netezza_performance_portal	The (1) ssl.conf and (2) httpd.conf files in the Apache HTTP Server component in IBM Netezza Performance Portal 2.0 before 2.0.0.4 have weak SSLCipherSuite values, which makes it easier for	2014-03-26	3.5	CVE-2014-0848

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.			
ibm -- lotus_protector_for_mail_security	Cross-site scripting (XSS) vulnerability in the Admin Web UI in IBM Lotus Protector for Mail Security 2.8.x before 2.8.1-22905 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2014-03-25	3.5	CVE-2014-0884
ithoughts -- ithoughtshd	Cross-site scripting (XSS) vulnerability in the iThoughtsHD app 4.19 for iOS on iPad devices, when the WiFi Transfer feature is used, allows remote attackers to inject arbitrary web script or HTML via a crafted map name.	2014-03-26	2.6	CVE-2014-1826
linux -- linux_kernel	Use-after-free vulnerability in the skb_segment function in net/core/skbuff.c in the Linux kernel through 3.13.6 allows attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphaning operation.	2014-03-24	2.9	CVE-2014-0131
linux -- linux_kernel	Use-after-free vulnerability in the nfqnl_zcopy function in net/netfilter/nfnetlink_queue_core.c in the Linux kernel through 3.13.6 allows attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphaning operation. NOTE: the affected code was moved to the skb_zerocopy function in net/core/skbuff.c before the vulnerability was announced.	2014-03-24	2.9	CVE-2014-2568
moodle -- moodle	Cross-site scripting (XSS) vulnerability in the quiz_question_tostring function in mod/quiz/editlib.php in Moodle through 2.3.11, 2.4.x before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote authenticated users to inject arbitrary web script or HTML via a quiz question.	2014-03-24	3.5	CVE-2014-2571
mozilla -- firefox	Mozilla Firefox before 28.0.1 on Android processes a file: URL by copying a local file onto the SD card, which allows attackers to obtain sensitive information from	2014-03-25	1.9	CVE-2014-1515

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the Firefox profile directory via a crafted application.			
openstack -- compute	The VMWare driver in OpenStack Compute (Nova) 2013.2 through 2013.2.2 does not properly put VMs into RESCUE status, which allows remote authenticated users to bypass the quota limit and cause a denial of service (resource consumption) by requesting the VM be put into rescue and then deleting the image.	2014-03-25	2.3	CVE-2014-2573

[Back to top](#)